

CLAIMS

What is claimed is:

1. A method for protecting a computer network from vulnerabilities, comprising:

 quarantining a computer system seeking to connect to said computer network until
 said quarantined computer system is remediated; and

 upon completing remediation of said quarantined computer system, connecting said
 remediated computer system to said computer network.
2. The method of claim 1, wherein said quarantine of said computer system is self-initiated.
3. The method of claim 2, wherein said remediation of said computer system is performed by
said computer network.
4. The method of claim 1, wherein said quarantining of said computer system seeking to
connect to said computer network further comprises:

 said computer system raising a firewall for blocking traffic between said computer system
and said computer network.
5. The method of claim 4, wherein said firewall permits a flow of vulnerability resolution
information therethrough.

6. The method of claim 5, and further comprising lowering said firewall after said computer system has been remediated using said vulnerability resolution information.

7. For a computer network comprised of a plurality of computer systems and a client remediation server coupled to each one of said plurality of computer systems, said client remediation server remediating said computer network by resolving vulnerabilities in said plurality of computer systems, a method for protecting said remediated computer network from unresolved vulnerabilities, comprising:

if one of said computer systems of said remediated computer network is disconnected from said remediated computer network, upon a subsequent re-connection of said computer system to said remediated computer network, temporarily limiting exchanges between said remediated computer network and said computer systems.

8. The method of claim 7, wherein exchanges between said computer system and said remediated computer network are limited until said computer system has been checked, by said client remediation server, for pending remediations.

9. The method of claim 8, wherein limiting exchanges between said computer system and said remediated computer network further comprises said computer system raising a firewall upon reconnecting to said remediated computer network.

10. The method of claim 9, wherein said computer system raising a firewall upon reconnecting to said remediated computer network further comprises filtering out non-remediation-related traffic between said computer system and said remediated computer network.

11. The method of claim 10, and further comprising removing said limitations on exchanges between said computer system and said remediated computer network upon said client remediation server executing said pending remediations for said computer system.

12. The method of claim 11, wherein removing said limitations on exchanges between said computer system and said remediated computer network further comprises said computer system lowering said firewall.

13. The method of claim 12, wherein removing said limitations on exchanges between said computer system and said remediated computer network further comprises permitting non-remediation-related traffic to pass between said computer system and said remediated computer network without filtering.

14. A method for protecting a computer network from nefarious software associated with a computer system being connected to said computer network, comprising:

upon initiating a connection between said computer system and said computer network,
quarantining said computer system from said computer network;

performing a scan on said computer system;

lifting said quarantine of said computer system upon completing the removal of any nefarious software detected by said scan.

15. The method of claim 14, wherein said computer system is quarantined from said computer network by a firewall residing on said computer system.

16. The method of claim 15, wherein said nefarious software detection and removal is performed by said computer network.

17. The method of claim 15, wherein said nefarious software detection and removal is performed by said computer system.

18. The method of claim 15, wherein said firewall permits traffic between said computer system and said computer network if said traffic is related to said nefarious software detection and removal.

19. The method of claim 18, wherein said nefarious software is a computer virus.
20. The method of claim 18, wherein said nefarious software is a worm.
21. A remediated computer network comprising:
- a computer system; and
- a client remediation server coupled to said computer system, said client remediation server configured to periodically resolve vulnerabilities in said computer system;
- wherein said computer system includes a firewall for periodically isolating said computer system, from said remediated computer network, until said client remediation server resolves vulnerabilities of said computer system.
22. The apparatus of claim 21, wherein said computer system is configured to raise said firewall to isolate said computer system from said remediated computer network whenever said computer system disconnects from and subsequently reconnects to said computer network.
23. The apparatus of claim 22, wherein said computer system is configured to raise said firewall upon each power-up thereof.

24. The apparatus of claim 22, wherein said remediated computer network is a local area network (LAN) and said computer system is configured to raise said firewall upon initiating registration with said LAN.

25. The apparatus of claim 22, wherein said remediated computer network is a wide area network (WAN) and said computer system is configured to raise said firewall upon initiating registration with said WAN.

26. The apparatus of claim 22, wherein said remediated computer network is a wireless local area network (WLAN) and said computer system is configured to raise said firewall upon initiating registration with said WLAN.

27. The apparatus of claim 22, wherein said remediated computer network is a virtual private network (VPN) and said computer system is configured to raise said firewall upon initiating registration with said VPN.

28. The apparatus of claim 22, wherein said remediated computer network is a wireless virtual private network (WVPN) and said computer system is configured to raise said firewall upon initiating registration with said WVPN.

29. The apparatus of claim 22, wherein said remediated computer network is the Internet and said computer system is configured to raise said firewall upon initiating registration with the Internet.

30. A computer system, comprising:

a processor subsystem;

a memory subsystem coupled to said processor subsystem;

at least one application residing in said memory subsystem and executable by said processor subsystem; and

a firewall switchable between a closed position in which traffic to and/or from said computer system is restricted and an open position in which traffic to and/or from said computer system is unrestricted;

wherein said firewall is configured to switch into said closed position upon power-up of said computer system and upon initiation of registration with a computer network.

31. The computer system of claim 30, wherein said firewall is configured to pass, in said closed position, first and second types of traffic, said first type of traffic being related to registration of said computer system with said computer network and said second type of traffic being related to remediation of said computer system by a client remediation server coupled to said computer network.